UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA v. (1) WEMERSON DUTRA AGUIAR, (2) PRISCILA BARBOSA, (3) EDVALDO ROCHA CABRAL, (6) GUILHERME DA SILVEIRA, (8) LUIZ NARCISO ALVES NETO, (10) ALTACYR DIAS GUIMARAES NETO, (11) ITALLO FELIPE PEREIRA DE SOUSA CORREA, (12) JULIO VIEIRA BRAGA, (13) PHILIPE DO AMARAL PEREIRA, (14) BRUNO PROENCIO ABREU, (16) ALESSANDRO FELIX DA FONSECA, and (18) SAULO AGUIAR PONCIANO Defendants	Criminal No. 1:21-cr-10158-MLW

GOVERNMENT'S CONSOLIDATED SENTENCING MEMORANDUM

RACHAEL S. ROLLINS
United States Attorney

DAVID HOLCOMB
KRISTEN A. KEARNEY
Assistant United States Attorneys

INTRODUCTION

Children have been cautioned for generations not to get into cars with strangers. Rideshare and delivery services offer a modern corollary. When a company like Uber or Lyft sends a driver to fetch a passenger, or a company like DoorDash or Instacart sends a driver to deliver food to a customer's door, the company is expected not to send any random person. Both the company's customers and the local authorities that permit the company to operate require the company to vet the driver as a matter of public safety.

The defendants are responsible for a widescale flouting of these requirements and expectations. They participated in mass identity theft for the sake of a massive fraud: by stealing personal identifiers of thousands of individuals, they created thousands of fraudulent driver accounts with the companies, to be used by other individuals who hoped to drive for one of the companies but were ineligible to do so. To the companies, their regulators, and their customers, these individuals were complete strangers.

A period of incarceration that accounts for the full scope of the fraud on customers and the identity theft that enabled it is required to deter further criminal activity of this kind. Because of the defendants' conduct, customers unknowingly paid millions of dollars for rides or deliveries from drivers who had not been subjected to even a basic level of vetting. Some of those millions reached the defendants, through payments from the companies; additional sums found their way to others whose activity the defendants enabled, and only a shadow of those amounts are reflected in payments that those other individuals sent to defendants. In most cases, defendants accomplished the fraud through the transfiguration of stolen identifiers and driver photographs

into purportedly real driver's license images that could pass automated checks. The sentences imposed on the defendants who orchestrated this fraud should account for these elements.[1]

BACKGROUND

The defendants have pleaded guilty to a nationwide conspiracy to obtain money by faking rideshare and delivery companies into allowing certain individuals to drive for the companies under other individuals' names. Some actively created the fraudulent accounts and rented and sold them to ineligible drivers. Others helped by stealing driver's license information and Social Security numbers, or by editing driver's license images to bear the photograph of the end user of the fraudulent account. To generate additional income from fraudulent accounts, some defendants used technology, like "bots" and GPS "spoofing," to claim more profitable deliveries or to make trips look longer than they actually were. Still others generated large referral bonuses from the companies—sometimes as high as $1,000 per account—to "refer" other fraudulent accounts to the companies' platforms. Regardless of a defendant's specific activity or combination of activities, the goal was the same: to make money by pretending to be someone else, or by helping others do the same.

For defendants to succeed—both in terms of meeting demand for accounts and keeping pace with companies' efforts to shut down fraudulent accounts—they required a pool of real individuals' personal identifiable information ("PII") to use to create fraudulent accounts. Defendants obtained this PII through various means as savvy as finding Social Security numbers

[1] With respect to restitution, the government respectfully submits that, in this case, "the number of identifiable victims is so large as to make restitution impracticable," and that "determining complex issues of fact related to the cause or amount of the victim's losses would complicate or prolong the sentencing process to a degree that the need to provide restitution to any victim is outweighed by the burden on the sentencing process." 18 USC § 3663A(c)(3)(A) and (B). The company victims in this case have indicated that they are not seeking restitution, and no identified individual victim has indicated that he or she will seek restitution.

for sale on the DarkNet or as simple as taking a photograph of a delivery customer's driver's license. The defendants also needed continuously to find ways around the fraud detection systems of sophisticated and deep-pocketed companies. At a minimum, circumventing these systems meant providing valid PII that would pass one or more background checks and presenting images of driver's licenses sufficiently resembling authentic licenses, right down to the security features.

Defendants succeeded in this scheme by coordinating with co-conspirators both in the United States and Brazil and sharing not only PII and fraudulent accounts, but also information about how to wring more money from fraudulent accounts and how to avoid getting shut down by the companies. One defendant single-handedly created thousands of fraudulent accounts. For some of these, she used driver's license images that other co-defendants obtained by duping recipients of alcohol deliveries into permitting the co-defendants to photograph their licenses. Several defendants worked with uncharged co-conspirators located in Brazil to manage and distribute fraudulent accounts and collect rental payments. Some defendants learned to edit driver's license images, while others farmed that work out to editors in Brazil. Most obtained Social Security numbers directly or indirectly through the DarkNet. Bridging these various actions was an agreement to make money by getting themselves and other people behind the wheel under other people's names.

The defendants have admitted to a scheme with staggering consequences. Countless thousands of trusting customers were denied rides or deliveries from drivers who were vetted—as required by state public safety laws and regulations—because of the defendants' crimes. The companies unknowingly approved thousands of fraudulent driver accounts and paid out millions to drivers who used them. Behind these fraudulent accounts were thousands of stolen identities. More broadly, defendants' crimes have undermined the baseline trust that customers of the

companies' services muster every time they call for a car to get home at the end of the night or place a grocery order for home delivery.

ARGUMENT

I. THE DEFENDANTS' SENTENCES SHOULD ACCOUNT FOR THE FULL SCOPE OF THE FRAUDULENT ACTIVITY THEY CAUSED

In fashioning an appropriate sentence, courts consider the factors set forth in 18 U.S.C. § 3553(a), including the seriousness of the offense, the history and characteristics of each defendant, the need for the sentence imposed to constitute just punishment and provide for adequate deterrence, and the importance of avoiding unwarranted sentencing disparities among similarly situated defendants.

The government has considered these factors, along with other measures of culpability: foremost, the extent to which individual defendants actively participated in the fraud and contributed to its success, the extent to which they involved others in the fraudulent activity, and the magnitude of their effects on customers and the companies.

For each defendant, incarceration commensurate with the scope of his or her involvement—based on amounts customers paid for unauthorized rides or trips the defendants facilitated—appropriately reflects the seriousness of the fraud offense and provides just punishment. Likewise, the mandatory two-year sentence for aggravated identity theft underscores that harvesting and using PII should not be taken as lightly as defendants evidently took it here.

A. The Seriousness of the Offense: Fraud on Customers in a Heavily Regulated Industry and in a Market Predicated on Trust

As the government detailed in its memorandum on common sentencing issues (Dkt. 716), in its sur-reply (Dkt. 766), and at the common issues hearing on February 24, 2023, the national rideshare and delivery companies do not answer to consumer demand and preferences alone.

Rather, largely in response to public safety concerns, state and local regulators have enacted minimum requirements for drivers for the companies operating within their jurisdictions. Regulations specify driver eligibility requirements, such as minimum age and driving experience, as well as driver's license and Social Security requirements. Most fundamentally, the companies are required to conduct background checks of the individuals that the companies send to customers' doorsteps, including driver and criminal history checks. In some states, like Massachusetts, a public authority conducts an additional background check.

Riders and delivery customers understand that the companies are expected to know some baseline amount about the people driving for them. When customers open a company's app, they are assured that drivers have passed background checks. They are given a name, vehicle, and photograph for the driver. They often can see how long the person has been driving for the company and what the driver's average rating is. The experience is possible in the first place because of a trust on the part of customers that the people in the driver's seat or at their doorsteps have been determined to be qualified and safe.

The defendants' scheme turned this trust on its head. Background checks and eligibility requirements only serve their purposes if they screen the correct individuals. At its core, defendants' scheme assured that, in the case of every fraudulent account, the companies and regulators approved accounts for individuals who never actually drove for the companies, for the use of drivers who were never screened. The reason for this is clear; the users of the fraudulent accounts would not have passed background checks themselves.

The defendants developed a certain infrastructure and body of knowledge for accomplishing this. For example, one way the companies attempted to ensure that the people they were vetting were actually the ones driving was to require applicants to upload a photograph of

their driver's licenses. The companies' systems would detect licenses that did not appear authentic and reject them. Therefore, in addition to procuring real driver's license information, defendants also needed to present the companies with driver's license images of sufficient fidelity to fool a computer system. The defendants could not simply traffick in stolen driver's licenses. Defendants also altered and reproduced the driver's license images so they would both bear the image of the fraudulent account user and avoid detection by the companies' fraud detection systems. These methods included both digital editing of driver's license images and the physical reproduction of driver's licenses, in each case preserving the security features that authentic licenses bear.[2]

The result of the defendants' scheme was the proliferation of thousands of fraudulent accounts, used to provide thousands of unauthorized rides, for which customers paid millions of dollars. Those millions of dollars are an appropriate measure of harm in this case because the

[2] At the hearing on February 24, 2023, the parties addressed *United States v. Jones*, 551 F.3d 19, 25-26 (1st Cir. 2008) and its potential application to the specific facts of this case. It is unclear whether the holding in *Jones* precludes the Court from applying the enhancement under USSG § 2B1.1(b)(11)(A) or (B) in a case like this, in which the means of identification that are the subject of the aggravated identity theft charge (*i.e.*, the driver's license information) are distinct from one or more authentication features used, possessed, trafficked, or produced (*e.g.*, holograms, watermarks, embossed text, or duplicate photographs) or even the access device trafficked (*e.g.*, the uploaded image depicting an altered driver's license).

Even if the First Circuit's holding in *Jones* limits the Court to applying the enhancement in cases of the *production* of unauthorized access devices and/or authentication features, there is sufficient basis to conclude that defendants produced both access devices and authentication features. *See* Affidavit of Special Agent Terrence Dupont (March 1, 2023). For example, defendant Aguiar recorded a video displaying an image of a driver's license printed one-sided on paper, which replicated the watermarks and embossed text on Massachusetts driver's licenses. *Id.*, Ex. A. Defendant Barbosa recorded several videos demonstrating how to use a computer program to edit the driver's photograph into the place of the duplicate, black-and-white photograph that California driver's licenses feature. *Id.*, Ex. B, Ex. C, Ex. D. Additionally, Barbosa used a "Badgy 100" card printer (https://us.badgy.com/printers/) at her residence to print edited driver's licenses. *Id.*, Ex. E. Whereas all defendants relied on altered driver's license images to engage in or facilitate fraudulent rideshare activity, these practices were reasonably foreseeable to them.

customers would not have ordered those rides or deliveries had they known that the drivers were not the authorized individuals that both companies and customers expected them to be. Generally, the more active a defendant was in the fraudulent scheme—whether through renting out fraudulent accounts, sourcing PII to create accounts, generating referral bonuses with fraudulent accounts, inflating the returns on fraudulent accounts with bots or GPS spoofing, or merely completing trips or deliveries with fraudulent accounts—the more money the defendant's activity generated for the defendant. This is true whether the defendant received that money directly from the companies or from others who received the money from the companies; in either case, those receipts reflect losses to unknowing customers.[3]

[3] In its memorandum, in its sur-reply, and at the hearing on February 24, 2023, undersigned counsel for the government stated that loss amounts determined by the Court should include certain Zelle payments to defendants, because these amounts more likely than not represented further loss to customers from the fraudulent scheme. This is so because the evidence generally shows that the defendants had few or no other legitimate sources of income; the defendants rented or sold fraudulent accounts to others, who paid them in Zelles; and the renters or purchasers of accounts who paid the defendants in Zelles themselves received payments for completed trips or deliveries from the companies. Counsel described how the Zelle inflows represent at least two underestimations of loss; payments from companies already underestimate amounts paid by the customers, and payments by account renters or purchasers excludes amounts earned in excess of that payment or rental price. Counsel acknowledged that the Zelle payments may represent other transactions, such as the purchase of stolen PII, the purchase of a bot, or the splitting of a referral bonus.

Because excluding Zelle inflows vastly understates total losses caused by defendants, the government maintains that the loss amount determined by the Court should reflect at least some portion of these amounts. The amounts of Zelles received by defendants who pleaded guilty without a plea agreement are summarized in the attached Affidavit of Forensic Accountant John Harger (March 1, 2023), with bank statements for those defendants attached. Defendants who pleaded guilty pursuant to plea agreements agreed to loss ranges reflecting a portion of their Zelle receipts. If the Court determines that available information is insufficient to support the inclusion of Zelles in the defendant's loss amounts, the government respectfully submits that the Court should still consider the Zelle receipts and depart upward under Application Note 21 to USSG § 2B1.1 on the basis of uncaptured losses caused by the defendants.

B. The Defendants' History and Characteristics

Each of the defendants is situated somewhat differently, and the government will address their individual backgrounds and characteristics more fully at their respective sentencing hearings. The defendants do have many common traits, though: most came to the United States from Brazil on temporary visas that have since expired, and most looked to an online community of Brazilian nationals living in the United States for work opportunities. They come from a variety of backgrounds and educational levels, but many had degrees or work experience in technical jobs. And they all, to some degree or another, became more active participants in the illicit market for fraudulent accounts with the major rideshare or delivery companies.

The defendants and their co-conspirators likely could not have remained and worked in the United States without work authorizations that they did not have, so they resorted to opportunities available to them to make money through fraudulent activity in the gig economy. While the perceived necessity of working in the United States in this way explains much of the fraudulent activity, it does not excuse it. Defendants took advantage of their Brazilian community members in the United States by making money from renting or selling those community members fraudulent accounts and, in the process, involving those community members in fraudulent activity. It is no answer that many drivers using the defendants' fraudulent accounts performed trips identically to non-fraudulent drivers; the defendants are not entitled to second guess the determinations or risk tolerances of regulators or customers. In short, the defendants seized opportunities to make money by circumventing public safety requirements to permit other ex-pats in the United States to make money. Honorable as the defendants may think their motives were, the upshot of their activity was widespread fraud.

The defendants may face immigration consequences, including possible deportation, as a result of their crimes. While the court may consider this eventuality "as part of a broader assessment of [defendants'] history and characteristics pursuant to section 3553(a)(1)[,]" *United States v. Hercules*, 947 F.3d 3, 9 (1st Cir. 2020), this is not one of the "relatively rare circumstances" in which that possibility should be given weight, *id.* at 10. First, as is clear from the Presentence Reports, most of the defendants had overstayed their visas by the time of their arrest and were already removable from the United States.[4] While criminal convictions may make those defendants' removable likelier, the convictions are only an additional impediment to continued residence in the United States. Second, it is not a foregone conclusion that the defendants will in fact be deported after serving a prison term. *Id.* at 8 ("Given the substantial possibility of shifting immigration policies and fluctuating enforcement priorities during [defendant's] incarcerative term, the district court's determination that the [defendant's] future deportation was not a matter of absolute certainty was a reasonable assessment of the [defendant's] circumstances."). More broadly, collateral consequences like potential deportation are "difficult to assess inasmuch as every defendant potentially faces wide-ranging repercussions as a result of a federal criminal conviction" including "difficulty securing employment and strained personal and family relationships[.]" *Id.* at 6 (summarizing district court's conclusions).

D. <u>The Avoidance of Unwarranted Sentencing Disparities</u>

The primary risk of sentencing disparities in this case stems from the different ways in which defendants caused losses to customers in the scheme. Deposits defendants received directly from the companies are more readily ascertainable. However, as addressed in the government's

[4] Exceptions include Barbosa, who obtained permanent resident status based on a sham marriage, and Cabral, who resided in the United States on a student visa at the time of his arrest.

memorandum on common issues, Dkt. 716 at 15-21, and in its sur-reply, Dkt. 766 at 5-6, other losses caused by defendants are not captured without reference to defendants' Zelle receipts, based on the information available about this widespread scheme. Because different defendants obtained money from the scheme in different ways, consideration of only deposits from the companies would result in the disparate sentencing of equally or near-equally culpable defendants. Specifically, excluding Zelle transfers from consideration would give undue benefit to defendants who rented or sold accounts to others, provided driver's license images or Social Security numbers used in creating fraudulent accounts, sold bots to be used in connection with fraudulent accounts, and/or received a cut of a referral bonus, to the extent those defendants received Zelles for their activities. Those activities also caused significant losses to customers and should be appropriately weighed in assessing a defendant's overall relative culpability.

Additionally, the need to avoid unwarranted disparities also cautions against consideration of a defendant's potential deportation, "when comparable arguments about immigration status 'would not be available' to a similarly situated citizen-defendant." *Hercules*, 947 F.3d at 6 (summarizing district court's reasoning).

E. <u>The Need for Specific and General Deterrence and Just Punishment</u>

These particular defendants pose a risk of reoffending. They committed the present offenses while in the United States with tenuous or non-existent authorization and with few work prospects. Their legal status in the country and work prospects are unlikely to improve following a prison sentence. Through the scheme, the defendants developed a niche expertise in obtaining stolen PII and finding evolving ways to beat companies' fraud detection systems. These skills are not readily translatable into lawful activity. Moreover, defendants' coordination with co-conspirators in Brazil illustrates that, even if they are deported to Brazil, defendants can continue

to lend their unique talents toward crime in the United States. Incarceration therefore is the best and surest way to deter these defendants in the future.

Incarcerative sentences reflecting the full scope of harm caused by these defendants will also effectively deter similarly situated individuals tempted to seek profit through mass identity theft and fraud in the gig economy. The investigation revealed the widespread use of Brazilian WhatsApp group chats to connect unauthorized drivers in the United States with fraudulent account creators. There is no reason to believe that this activity is limited to members of the Brazilian community. The sentences in this case should make clear to participants in those illicit markets that they risk significant consequences by stealing identities and imposing unauthorized services on unsuspecting customers for money.

II. INDIVIDUAL SENTENCING RECOMMENDATIONS

Beyond properly reflecting the gravity of the offense and the other factors in Section 3553(a), the defendants' sentences should also account for relative culpability within the group. What follows is a short summary of each defendant's offense conduct and a table setting forth the government's sentencing recommendations.

A. The Offense Conduct

All of the defendants facilitated significant use of fraudulent driver accounts to defraud customers and make money. Set forth below is a brief synopsis of each defendant's conduct.

i. *Wemerson Dutra Aguiar*

Aguiar bought and sold driver's license images and Social Security numbers and created hundreds of fraudulent driver accounts that he rented and sold. In the process, he worked with co-defendants Correa, A. Neto, L. Neto, Prado, Pereira, and Barbosa, among others. For example, he purchased driver's license images and Social Security numbers from Prado and Correa. He later

sold Social Security numbers to Prado and L. Neto. Aguiar paid A. Neto for edited images of driver's licenses. He split the proceeds of accounts he created with Pereira in exchange for Pereira referring drivers to him and managing the accounts. And he exchanged a driver's license template with Barbosa.

Aguiar regularly advertised the accounts he had created for rent or sale on WhatsApp. He also exchanged advice on how to circumvent the rideshare and delivery companies' fraud detection systems, shared contacts for individuals who could edit license images, gave advice on whether others' edits (such as Correa's) would make it past the companies' security, and aided others in troubleshooting account closures. Aguiar also rented cars to the individuals buying or renting the fraudulent driver accounts he created.

In connection with the scheme, Aguiar caused a loss of at least $100,705 from accounts in at least 25 other individuals' names.[5] This amount does not account for approximately $218,795 in Zelle deposits which correspond to rental or purchase payments for fraudulent accounts, car rental payments, and payments for Social Security numbers. Nor does it account for Zelle payments received from co-defendants Braga, Correa, Da Silva, Da Silveira, Pereira, and Prado.

ii. *Priscila Barbosa*

Barbosa created over 2,000 fraudulent driver accounts with multiple rideshare and delivery companies, which she rented, and sold. She advertised fraudulent accounts she created over WhatsApp group chats and typically rented them for between $200 and $300 per week. Barbosa created and managed accounts and split income with several partners, including Cabral, Da

[5] The government notes that this number is far short of the approximately 180 accounts Rideshare Company A has linked to Aguiar through various metadata and the more than 500 images of victims' driver's licenses found through a court-authorized search of Aguiar's iCloud account.

Silveira, and an uncharged co-conspirator referenced in the Second Superseding Indictment as "CC-1."

Barbosa used driver's license images provided by Cabral, who obtained them from the DarkNet; from co-defendants Abreu and Oliver Felipe Gomes De Oliveira, who obtained them while making alcohol deliveries; and from others. In some cases, Barbosa used a license editor to photo-edit photographs information onto the stock license images. Barbosa edited the licenses for her fraudulent accounts and provided edited or unedited licenses for others who created their own accounts, including Cabral and co-defendant Ponciano. Barbosa purchased Social Security numbers, typically for $100 each, from other co-conspirators who obtained the numbers on the DarkNet. She also sold Social Security numbers to Ponciano and co-defendant Placido.

Barbosa generated referral bonuses from Delivery Company D by "referring" new fraudulent accounts she created to the company. Barbosa obtained information about obtaining higher bonuses from Placido, and she split referral bonuses with Da Fonseca, who managed the individuals driving under the accounts and hitting the delivery targets to generate the bonuses.

Barbosa created a WhatsApp group chat that she named "Mafia." This group, which included co-defendants Cabral, Da Silveira, Ramos, Placido, and Abreu, as well as CC-1, shared tips to troubleshoot issues with account openings or closures, alerted each other about new policies from the rideshare and delivery companies and problematic customers to avoid, and provided information about available referral bonuses. Group members also pooled resources to purchase a bot to sell to users of fraudulent accounts.

In connection with the scheme, Barbosa caused a loss of at least $284,429 from accounts in numerous other individuals' names. This amount does not account for approximately $505,751 in Zelle deposits which correspond to rental or purchase payments for fraudulent accounts,

payments for driver's license images and Social Security numbers, and split referral bonuses. Nor does it account for Zelle payments received from other co-defendants.

iii. *Edvaldo Rocha Cabral*

Cabral created fraudulent driver accounts with various rideshare and delivery companies and advertised them on various social media sites, including WhatsApp and Facebook, and at a store in Everett frequented by Brazilians. To create the accounts, he purchased driver's license images and Social Security numbers from the DarkNet and paid others to edit the driver's license images for him.

After Cabral met Barbosa at a party, he partnered with her to create fraudulent driver accounts. Cabral purchased driver's license images from Barbosa, and also supplied her with Social Security numbers. Cabral advertised the accounts Barbosa created with the driver's license images and Social Security numbers they obtained, and they split the proceeds. They also worked together to generate referral bonuses and shared the license editor.

In June 2020, Barbosa added Cabral to the "Mafia" chat group. As a member of this chat group, Cabral agreed to purchase a "bot" to claim the most profitable deliveries from Delivery Company E's app, which he then sold to drivers along with the fraudulent accounts.

In connection with the scheme, Cabral caused a loss of at least $27,914 from accounts in at least 3 other individuals' names. This amount does not account for approximately $355,570 in Zelle deposits which correspond to rental or purchase payments for fraudulent accounts, payments for driver's license images and Social Security numbers, and split referral bonuses. Nor does it account for Zelle payments received from Barbosa.

iv. *Guilherme Da Silveira*

Within months of arriving in the United States, Da Silveira began participating in the

scheme by renting fraudulent rideshare driver accounts. Shortly thereafter, he partnered with co-defendant Barbosa to create, rent, and sell driver accounts. Da Silveira's role was to obtain images of victims' driver's licenses, which he then shared with Barbosa who created the fraudulent driver accounts using the victims' identities.[6] Da Silveira then found individuals to buy or rent the accounts via WhatsApp group chats targeted toward the Brazilian community in the United States. Da Silveira also rented cars to the individuals buying or renting the fraudulent driver accounts.

After the onset of the COVID-19 pandemic, Da Silveira expanded to fraudulent delivery driver accounts. He continued to obtain victims' driver's licenses, and additionally purchased victims' Social Security numbers, in order to create accounts and obtain fraudulent referral bonuses. In June 2020, Barbosa added Da Silveira to the "Mafia" chat group. As a member of this chat group, Da Silveira agreed to purchase a "bot" to claim the most profitable deliveries from Delivery Company E's app, which he then sold to drivers along with the fraudulent accounts. Da Silveira also utilized "GPS spoofing" to fake his location on the rideshare and delivery companies' apps.

In connection with the scheme, Da Silveira caused a loss of at least $284,578 from accounts in at least 37 other individuals' names. This amount does not account for approximately $223,380 in Zelle deposits which correspond to rental or purchase payments for fraudulent accounts, car rental payments, and payments for the Delivery Company E "bot." Nor does it account for Zelle payments received from Barbosa for their shared accounts, as well as payments Da Silveira received from co-defendant Ponciano.

[6] Da Silveira also sold driver's license images to an unindicted co-conspirator, who in turn sold them to co-defendant Aguiar.

v. *Luiz Narciso Alves Neto*

L. Neto met co-defendants Da Silva and Prado while driving for the rideshare companies at Logan Airport. He rented fraudulent accounts for $250 to $300 per week from Da Silva, who created fraudulent accounts with individuals in the United States and Brazil. He also was given accounts to use by Prado, who rented fraudulent accounts that he created over Brazilian WhatsApp group chats. On at least one occasion, L. Neto purchased a Social Security number from Aguiar.

L. Neto sold "bots" that allowed users to claim the most profitable orders from Delivery Company E's app. Prado referred his account renters and purchasers to L. Neto to buy the bot, and L. Neto sold those individuals used Android phones with the bot already installed for $500 to $600. L. Neto split proceeds from bot sales with Prado. He also instructed others on how to use the bot.

In connection with the scheme, L. Neto caused a loss of at least $66,354 in connection with fraudulent accounts in the names of at least three other individuals. This amount does not account for approximately $76,113 in Zelle deposits which correspond to payments for the Delivery Company E "bot" and other payments related to fraudulent accounts. Nor does it account for Zelle payments received from co-defendants.

vi. *Altacyr Dias Guimaraes Neto*

In addition to renting and selling fraudulent driver accounts, A. Neto arranged for driver's license image editing for others, including co-defendant Aguiar. A. Neto also purchased driver's licenses from Aguiar, which he used to create his own fraudulent accounts that he then rented and sold. In their communications, A. Neto and Aguiar exchanged tips on how to circumvent the rideshare and delivery companies' fraud detection systems, in particular their facial recognition technology. A. Neto also rented cars to the individuals buying or renting the fraudulent driver

accounts.

In connection with the scheme, A. Neto caused a loss of at least $162,399 from accounts in at least 40 other individuals' names. This amount does not account for approximately $192,295 in Zelle deposits which correspond to rental or purchase payments for fraudulent accounts, car rental payments, and payments for edited driver's license images. Nor does it account for Zelle payments received from Aguiar or co-defendant Cabral for editing licenses.

vii. *Itallo Felipe Pereira de Sousa Correa*

Correa first became involved in the scheme through his rental or purchase of fraudulent driver accounts for his own use, including from co-defendant Aguiar. Later, Correa expanded his involvement by creating accounts for others to rent or buy, including his former roommate and co-defendant Braga. To create these accounts, Correa purchased Social Security numbers from Aguiar that corresponded to driver's licenses Correa obtained from another source. As Correa became more deeply involved in the scheme, he began obtaining Social Security numbers for Aguiar, rather than relying on Aguiar to supply them to him. Correa also sold driver's license images to another co-conspirator, through Aguiar. Additionally, Correa originally outsourced the editing of driver's license images, but later began editing them himself and relied on Aguiar to provide feedback on whether his edits would get past the rideshare and delivery companies' fraud detection systems.

Correa also purchased and used a GPS spoofing app and instructed Aguiar on how to use it. Correa discussed with Aguiar expanding his account creation activity from California into the Massachusetts market. To conceal the extent of his scheme, Correa used Braga's bank account to receive payments from the rideshare and delivery companies and individuals renting or purchasing accounts Correa created.

In connection with the scheme, Correa caused a loss of at least $139,186 from accounts in at least 51 other individuals' names. This amount does not account for approximately $144,045 in Zelle deposits which correspond to rental or purchase payments for fraudulent accounts, among other things. Nor does it account for Zelle payments received from Braga for use of Braga's bank account or Aguiar for the purchase of driver's license images and Social Security numbers.

Upon learning of the arrests of co-defendants in this case, Correa fled the United States with Braga by driving to the Mexican border. From there, he attempted to fly to Brazil, which does not extradite its own citizens, but was apprehended at a layover in Panama.

viii. *Julio Vieira Braga*

Shortly after his arrival in the United States, Braga began renting or buying fraudulent driver accounts for his own use. Later, Correa, who was Braga's roommate at the time, brought Braga into the larger conspiracy. In exchange for Correa providing Braga with accounts to drive under, Braga allowed Correa to use Braga's bank account in connection with Correa's buying and selling driver's licenses and Social Security numbers, editing of license images, and managing, renting, and selling fraudulent driver accounts. Correa also introduced Braga to co-defendant Aguiar, from whom Braga rented a fraudulent driver account in November 2019. In their communications, Braga attempted to go even deeper into the scheme by offering Aguiar the contact information for someone to edit licenses for Aguiar. Still later, Braga attempted to create his own fraudulent accounts based on driver's licenses he had obtained while making alcohol deliveries.

In connection with the scheme, Braga caused a loss of at least $115,203 from accounts in at least 32 other individuals' names. This amount does not account for approximately $59,885 in Zelle deposits which correspond to, among other things, rental or purchase payments for fraudulent

accounts. Nor does it account for Zelle payments received from Correa.

Upon learning of the arrests of co-defendants in this case, Braga fled the United States with Correa by driving to the Mexican border. From there, he attempted to fly to Brazil, which does not extradite its own citizens, but was apprehended at a layover in Panama.

ix. *Philipe do Amaral Pereira*

Like many of his co-defendants, Pereira began driving for rideshare companies shortly after his arrival in the United States, although initially under his true identity. However, when those accounts were closed because Pereira did not meet their eligibility requirements, Pereira began to rent fraudulent driver accounts in victims' names for his own use. Thereafter, he met Aguiar through a WhatsApp chat group for members of the Brazilian community in the United States. Pereira began operating as a middleman between Aguiar, who created fraudulent driver accounts, and drivers interested in driving under those accounts. Pereira gathered individuals' pictures, vehicle, insurance, and bank information and provided it to Aguiar, who in turn created accounts under victims' identities but using the photos, vehicle, insurance, and bank information that Pereira had provided. Once these fraudulent driver accounts were opened, Pereira served as a resource for the drivers if they had account problems, and also collected payments from drivers who rented accounts. If a driver was late in paying, Pereira reported the driver to Aguiar, who would change the password on the account to prevent the driver from accessing it until the driver paid up. Pereira received a commission of approximately $50 per account per week for making these arrangements between the drivers and Aguiar, plus a kickback of $40 per account from Aguiar for each account opened.

In addition to the accounts for which he served as a middleman, Pereira also arranged for Aguiar to create a fraudulent driver account for Periera to use. Pereira obtained the driver's license

image for this account after a traffic accident, in which Pereira took a photo of the license of the person that hit him. Pereira sent this driver's license to Aguiar and asked Aguiar to track down the corresponding Social Security number. Aguiar offered to split the profits from this account with Pereira.

In connection with the scheme, Pereira caused a loss of at least $42,483 from accounts. This amount does not account for approximately $74,910 in Zelle deposits which correspond to rental or purchase payments for fraudulent accounts from the individuals for whom Pereira served as the middleman to Aguiar. Nor does it account for Zelle payments received from Aguiar.

x. *Bruno Proencio Abreu*

Abreu both created and rented or sold fraudulent driver accounts and obtained more than 90 driver's licenses that he sold to Barbosa to create fraudulent driver accounts. Abreu worked as a delivery driver under fraudulently created accounts, and targeted alcohol deliveries, including by driving to a large liquor store in Connecticut to secure primarily alcohol deliveries. When making these deliveries, Abreu falsely told the recipient that he needed to scan their driver's license for the delivery application, even though this step was not required. Instead, Abreu took photos of the licenses for his own use and to sell to Barbosa. Barbosa used these licenses to create fraudulent driver accounts in the victims' names and split the proceeds from these accounts with Abreu.

Abreu also connected individuals looking for fraudulent driver accounts with Barbosa, who was also Abreu's roommate during part of the scheme. Abreu also helped Barbosa purchase Bitcoin, which she then used to purchase Social Security numbers on the Darknet. Barbosa also relied on Abreu to change the mailing addresses for fraudulent driver accounts such that the companies would not send tax forms to victims, thereby alerting them to the scheme. Always interested in expanding their scheme, Abreu also suggested to Barbosa that they work with an

accountant, whom he believed had access to individuals' Social Security numbers, or an insider at one of the rideshare and delivery companies, whom he believed could provide them with confidential information to prevent their fraudulent accounts from being shut down. As Barbosa's roommate, Abreu had access to the license printer located pursuant to a court-authorized search in a common area of the apartment. Additionally, during the search, investigators located three driver's licenses in victims' names in Abreu's bedroom, including one with Abreu's photo edited onto the license.

Separate from his work with Barbosa, Abreu created fraudulent driver accounts to rent or sell to others, including to collect referral bonuses. In connection with the scheme, Abreu caused a loss of at least $61,492 from accounts in at least 20 other individuals' names. This amount does not account for approximately $29,745 in Zelle deposits which correspond to, among other things, rental or purchase payments for fraudulent accounts. Nor does it account for more than $27,000 in Zelle payments received from Barbosa.

xi. ***Alessandro Felix Da Fonseca***

Within weeks of arriving in the United States, Da Fonseca began renting or buying fraudulent driver accounts for his own use, including an account he rented from co-defendant Barbosa, from whom he also rented a car. Later, Da Fonseca began working more closely with Barbosa to advertise fraudulent driver accounts that she had created via WhatsApp group chats targeted toward the Brazilian community in the United States and by word of mouth. Da Fonseca acted as an intermediary by passing individuals' names and bank account information to Barbosa, who would then create accounts for those individuals and provide the log-in information to Da Fonseca to share with the driver. Da Fonseca also purchased fraudulent driver accounts from Barbosa, and then rented them out to others.

Da Fonseca also worked with Barbosa to generate referral bonuses by finding drivers to complete a specified number of deliveries under a fake account Barbosa had "referred" to qualify for referral bonus payments. Da Fonseca monitored these drivers to ensure they completed the necessary number of deliveries within the time to earn the referral bonus, and when the drivers were in danger of missing the cutoff, Da Fonseca took over the accounts and completed the necessary number of deliveries himself to generate the bonus.

Da Fonseca also allowed Barbosa to use his address for receipt of debit cards associated with fraudulent driver accounts she created through Delivery Company D. When he received the debit cards, Da Fonseca took photos of them and sent the photos to Barbosa to link the cards to the fraudulent accounts she had created.

In connection with the scheme, Da Fonseca caused a loss of at least $128,522 from accounts in at least 27 other individuals' names. This amount does not account for approximately $54,715 in Zelle deposits which correspond to rental or purchase payments for fraudulent accounts, among other things. Nor does it account for Zelle payments received from Barbosa for his cut of their shared referral bonuses.

xii. *Saulo Aguiar Ponciano*

Ponciano created and rented out or sold his own fraudulent driver accounts in Massachusetts and in Illinois. Ponciano consulted Barbosa in connection with attempting to use a bot with Delivery Company E's app, and Barbosa offered Ponciano a bot for $500. Ponciano and Barbosa also discussed generating referral bonuses with Delivery Company D. Ponciano also relied on Barbosa to supply PII for his accounts. For example, in June 2020, he paid Barbosa $900 for Social Security numbers that Barbosa located for nine individuals whose driver's licenses Ponciano had messaged to Barbosa.

Ponciano rented and sold accounts to members of the Brazilian community in the United States. For example, Ponciano advertised a fraudulent account for rent via a Brazilian WhatsApp group in September 2020. In October 2020, Ponciano sold an account with Delivery Company B to an individual for $1,000.

In connection with the scheme, Ponciano caused a loss of at least $106,520 from accounts in at least 33 other individuals' names. This amount does not account for approximately $244,450 in Zelle deposits which correspond to rental or purchase payments for fraudulent accounts, among other things. Nor does it account for Zelle payments received from co-defendants Barbosa, Wanderly, Da Silveira, Ramos, A. Neto, and Cabral.

B. Sentencing Recommendations

For each defendant, the government's recommended sentence is near or below the low end of the Sentencing Guidelines as calculated by the parties (in the case of the nine defendants who signed plea agreements) or the government (in the case of the five defendants who did not sign plea agreements). For some defendants, the government's recommendation is also below what the government agreed to recommend as part of the relevant plea agreement. These recommendations are set forth in the following table. Each Guidelines Range and recommendation includes a 24-month mandatory sentence for aggravated identity theft.

Defendant	Guidelines Range (Plea Agreement or Gov't)	Final Sentencing Recommendation
Wemerson Dutra **AGUIAR**	75-87 months (Gov't)	75 months
Priscila **BARBOSA**	87-102 months (Plea Agreement)	53 months

Defendant	Guidelines Range (Plea Agreement or Gov't)	Final Sentencing Recommendation
Edvaldo Rocha **CABRAL**	75-87 months (Gov't)	75 months
Guilherme **DA SILVEIRA**	75-87 months (Plea Agreement)	59 months
Luiz Narciso **ALVES NETO**	65-75 months (Gov't)	65 months
Altacyr Dias **GUIMARAES NETO**	65-75 months (Plea Agreement)	57 months
Itallo Felipe Pereira de **SOUSA CORREA**	65-75 months (Plea Agreement)	54 months
Julio **VIERA BRAGA**	51-57 months (Plea Agreement)	36 months
Philipe do Amaral **PEREIRA**	45-51 months (Plea Agreement)	36 months
Bruno Proencio **ABREU**	57-65 months (Plea Agreement)	51 months
Alessandro Felix **DA FONSECA**	57-65 months (Gov't)	57 months
Saulo Aguiar **PONCIANO**	65-75 months (Gov't)	65 months

CONCLUSION

Defendants caused customers and riders to receive countless thousands of rides and deliveries from people who were not who they claimed to be. Each of these rides and deliveries rested on the theft of personal identifiers of others and contravened regulations meant to protect public safety. Defendants supplied the thousands of fraudulent accounts that made these unauthorized trips possible. The Court should hold them accountable for their disregard for the trust that customers place in authorized drivers when they climb into the backseat or open their front door.

Respectfully submitted,

RACHAEL S. ROLLINS
United States Attorney

By: */s/ David M. Holcomb*
KRISTEN A. KEARNEY
DAVID M. HOLCOMB
Assistant United States Attorneys

Date: March 1, 2023

CERTIFICATE OF SERVICE

I hereby certify that a true copy of the above document was served upon the attorney of record for each other party by CM/ECF on March 1, 2023.

/s/ David M. Holcomb
DAVID M. HOLCOMB